ABSTRACT OF THE DISCLOSURE

An objective of the present invention is to obtain a mutual authentication method in which mutual authentication is carried out securely and conveniently. In order to achieve the above objective, in the mutual authentication process, a private key K_0, being an initial value, is stored in a client and a server (Pc0, Ps0). The client generates a random number *R*, calculates secret data *C* and authentication data *A*, and transmits the data items to the server (Pc1). The server receives the authentication data *A* and the secret data *C* from the client, and generates a random number Q, calculates secret data *S*, and authentication data B and returns the data items, as well as updating the private key K_0 with a private key K_1 (Ps1). The client receives from the server the authentication data *B* and the secret data *S*, generates the random number *R*, calculates secret data C_2, authentication data A_2, and returns the data items to the server, and updates the private key K_0 with the private key K_1(Pc2). The client and the server check whether or not validity is established (Ps_{m+1}, Pc_{m+1}). Further in the authentication method above, there is a method for generating a onetime ID, assuming that the onetime ID is identification information usable just one time in the authentication between a plurality of devices or application. In each of the devices or applications which carries out the authentication, a variable shared key which changes per predefined communication unit requiring the authentication is generated, a function value of one-way function is obtained in which the variable

shared key is used as an argument, a onetime ID hard to tap and superior in security is generated based on the function value, and the onetime ID is utilized.